North Dakota Law Review

Volume 77 | Number 4 Article 6

2001

Statutes - Telecommunications - From CALEA to Carnivore: How Uncle Sam Conscripted Private Industry in Order to Wiretap Digital Telecommunications

Jason Broberg

STATUTES—TELECOMMUNICATIONS—FROM CALEA TO CARNIVORE: HOW UNCLE SAM CONSCRIPTED PRIVATE INDUSTRY IN ORDER TO WIRETAP DIGITAL TELECOMMUNICATIONS

U.S. Telecom Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000)

I. FACTS

In 1984, the federal government broke up AT&T.[1] Technological competition within the telecommunications industry was furious following the breakup.[2] Between 1984 and 1994 telecommunications technology, especially digital telecommunications technology,[3] advanced at unprecedented rates and law enforcement had not kept pace.[4] Congress wanted to ensure law enforcement had the technological ability to conduct telephonic surveillance; to that end, Congress conscripted the assistance of the telecommunications industry.[5] In the waning days of its 103d session, Congress enacted legislation mandating that private industry create and employ technologies to assist law enforcement in monitoring and capturing digital telecommunication information.[6] That legislation was the Communications Assistance for Law Enforcement Act of 1994 (CALEA).[7] CALEA required the telecommunication carriers to assist law enforcement in obtaining the content of digital telephone calls and information that may identify a call, such as a telephone number.[8]

Congress wanted uniform and efficient implementation of the legislation and therefore asked the telecommunications industry, rather than the Federal Communications Commission (FCC), to draft the administrative

---

1. Lillian R. BeVier, *Symposium Tribute to William F. Baxter, The Communication Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break up of AT&T*, 51 STAN. L. REV. 1049, 1050 (1999).

2. *Id.*

3. Digital telecommunications include wired telephony technologies such as fiber optics and computerized switching, mobile telephony technologies such as cellular and digital PCS (personal communication services), as well as the Internet and e-mail. In this case comment both cellular and digital PCS technologies are referred to with the umbrella terms "cellular" or "mobile" telephones.

4. BeVier, *supra* note 1, at 1050-51.

5. 47 U.S.C. § 1002 (1994 & Supp. V 1999).

6. BeVier, *supra* note 1, at 1051. President Clinton signed the Communications Assistance for Law Enforcement Act (CALEA) into law on October 25, 1994. *Id.* (citing Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended in scattered sections of 18 & 47 U.S.C. (1994 & Supp. V 1999))).

7. *Id.*

8. 47 U.S.C. § 1002(a) (1994).

implementation standards.[9] From 1995 until 1997, the Telecommunications Industry Association (TIA), which had assumed leadership for the telecommunications industry, consulted with the Federal Bureau of Investigation (FBI) to determine the CALEA implementation standards.[10] In the spring of 1997, the TIA asked telecommunication carriers and law enforcement agencies (LEAs) to vote on a proposed cellular and digital personal communications services (PCS) and wireline compliance standard.[11] The LEAs rejected the standard.[12]

In part, the LEAs voted against the plan because the FBI wanted nine capabilities beyond what the TIA offered.[13] The most controversial of the nine was the ability to capture the digits dialed after a call is connected.[14] This capability is called "post-cut-through digits" or "dialed digit extraction."[15] Beyond dialed digit extraction, the FBI wanted to know when a person joins or leaves a conference call and when the person uses call forwarding or call waiting.[16] The FBI asked for access to electronic signals indicating a telephone is ringing, is busy, or has a waiting call or message.[17] The FBI wanted to monitor the content of conference calls and have access to system timing records in order to match monitored call content to the system's various electronic signals.[18] Further, the FBI wanted the telecommunication carriers to verify that an established wiretap is functioning.[19] Telecommunication carriers were asked to inform law enforcement when a tapped telephone was in use and to indicate when a tapped customer was

9. 47 U.S.C. § 1006(a)(1) (1994).

10. Michael A. Rosow, Note, *Is Big Brother Listening? A Critical Analysis of New Rules Permitting Law Enforcement Agencies to Use Dialed Digit Extraction*, 84 MINN. L. REV. 1051, 1063 (2000).

11. *See In re* Communications Assistance for Law Enforcement Act, Further Notice of Proposed Rulemaking (*Further Notice*), ¶ 134, 13 F.C.C.R. 22,632, 22,690 (1998) (stating J-Standard applies only to wireline, cellular and PCS carriers); *Id.* ¶ 12 at 22,640 (noting that the balloting occurred in the spring of 1997).

12. *Id.* ¶ 12 at 22,640.

13. *See* Rosow, *supra* note 10, at 1063. Other LEAs wanted capabilities beyond those nine requested by the FBI; for example, the New York City Police Department wanted to use radio direction finding to determine the location in space where a cellular signal is originating. *In re* Communications Assistance for Law Enforcement Act, Third Report and Order (*Third Report*), ¶¶ 43 & 46, 14 F.C.C.R. 16,794, 16,815-16 (1999).

14. *Third Report*, ¶ 112 at 16,842. An example is the digits representing a bank account number, dialed after first connecting to the telephone number of a bank. *Id.* ¶ 119 at 16,844.

15. *Id.* ¶ 112 at 16,842.

16. *Id.* ¶¶ 68 & 76 at 16,825, 16,828.

17. *Id.* ¶ 83 at 16,830.

18. *Id.* ¶¶ 58 & 90 at 16,821, 16,833.

19. *Id.* ¶ 97 at 16,836.

adding or deleting calling features such as call waiting.[20] These nine capabilities are collectively known as "custom calling features."[21]

Congress had not required law enforcement participation in the balloting process; therefore, the telecommunication industry re-balloted without law enforcement participation and unanimously adopted the TIA proposal.[22] In December of 1997, the TIA published the adopted standards under the title, "Interim Standard/Trial Use Standard J-STD-025" (J-Standard).[23] However, even without the custom calling features, the J-Standard contained provisions that proved controversial to groups interested in digital privacy.[24]

For example, under the J-Standard, the telecommunications industry was to provide law enforcement the location of the cellular antenna used at the beginning and end of a targeted telephone call.[25] This provision was a compromise between the telecommunications industry and law enforcement.[26] Originally, law enforcement wanted the ability to track mobile telephones as they moved from cell site to cell site.[27] The New York City Police Department wanted to determine the precise physical location of the caller by plotting the direction from which cellular signals arrived at multiple antennas.[28] On the other hand, SBC Communications, Inc. wanted to provide only the location of the "landline central office" through which the cellular calls were routed.[29] Negotiations led to compromise, and the telecommunications industry agreed to provide the location of the antennas used at the beginning and end of a marked call.[30] There was also agreement that court authorization was required to access location information.[31]

---

20. *Id.* ¶¶ 102 & 107 at 16,838, 16,840.

21. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 463 (D.C. Cir. 2000).

22. *Further Notice*, ¶¶ 14-15, 13 F.C.C.R. 22,632, 22,642 (1998).

23. *Id.* ¶ 14.

24. *Third Report*, ¶ 13, 14 F.C.C.R. 16,794, 16,802 (1999); *see also In re* Communications Assistance for Law Enforcement Act, Public Notice (*Public Notice*), 13 F.C.C.R. 13,786 (1998) (articulating Center for Democracy and Technology's argument that it cannot reasonably comply with the interim standard, and its request that the FCC delay implementing the Act indefinitely).

25. *Third Report*, ¶ 44, 14 F.C.C.R. at 16,815.

26. *Further Notice*, ¶ 50, 13 F.C.C.R. at 22,656-57.

27. *Id.*

28. *Third Report*, ¶¶ 43 & 46, 14 F.C.C.R. at 16,815-16. This process is known as triangulation or, alternatively, as radio direction finding. *Id.*

29. *Further Notice*, ¶ 50, 13 F.C.C.R. at 22,656-57. SBC Communications is affiliated with Southwestern Bell Telephone. *Id.* at 22,708 (separate statement of Commissioner Harold W. Furchtgott-Roth).

30. *Third Report*, ¶ 44, 14 F.C.C.R. at 16,815.

31. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 458, 464 (D.C. Cir. 2000).

The J-Standard also provided "packet-mode" data to law enforcement.[32] Data packets are a technology new to the digital age.[33] With older communication systems, a single dedicated circuit opened between the callers.[34] Instead of delivering data in a continuous stream within a single circuit, digital technology breaks data into small bits and sends those bits through multiple circuits via numerous routes.[35] These packets re-assemble in sequence at the ultimate destination.[36] Because the data is broken down and re-assembled, each packet has addressing and sequencing information in addition to the data.[37] Often it is difficult to fully separate the addressing and sequencing data from the data forming the message.[38] US West and others objected that limiting law enforcement access to either the addressing information or the content was not currently possible because complete separation of the data is not possible.[39] The FBI disagreed and argued that such separation is technologically feasible.[40]

The FCC received three petitions for review of the J-Standard in the spring of 1998.[41] The Center for Democracy and Technology (CDT) asked the FCC to reject the antenna location information and packet-mode data portions of the J-Standard.[42] The CDT alleged that packet-mode data provided law enforcement with more capability than Congress envisioned by allowing law enforcement access to call content in situations where a court has approved access only to call identification information.[43] In another petition for review, the FBI and the Department of Justice argued that the J-Standard should include further assistance requirements and capabilities.[44] The FBI asked the FCC to add the nine surveillance capabilities for which

---

32. *Id.* at 464.

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.* The FCC invited further study of packet-mode data because of the risk that content could be obtained when law enforcement was only authorized to collect call-identification information. *Further Notice*, ¶¶ 64-66, 13 F.C.C.R. 22,632, 22,662-63 (1998). This constitutes a privacy concern because it would enable law enforcement to access private personal information, such as a bank account number, when it was only authorized to secure telephone numbers. *Id.*

39. *Third Report*, ¶ 53, 14 F.C.C.R. 16,794, 16,818 (1999). The FCC outlined the US West objection as follows, "separating the header from content in packet-mode communications is not feasible because packet data is delivered in a layered stack structure, and carriers have neither the ability nor any business reason to monitor packet data streams and then decipher the various protocols." *Id.*

40. *Id.* ¶ 54 at 16,818.

41. *Public Notice*, 13 F.C.C.R. 13,786 (1998).

42. *Id.*

43. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 456 (D.C. Cir. 2000).

44. *Public Notice*, 13 F.C.C.R. at 13,786.

the FBI previously asked the TIA.[45] In response to the CDT and FBI petitions, the TIA asked for a determination whether the J-Standard was either under-inclusive, as argued by the FBI, or over-inclusive, as asserted by the CDT.[46]

The CDT offered three separate arguments attacking the location information requirement.[47] First, location information would turn mobile phones into tracking devices.[48] Transforming private property into government surveillance devices, the CDT asserted, violated CALEA provisions that law enforcement was to have no more surveillance capabilities with digital technologies than the law tolerated with "plain old telephone service" (POTS).[49] The CDT pointed to CALEA language stating that the physical location of the marked telephone was not to be obtained via a "pen register" or "trap and trace device" as call identifying information except to the extent that the location could be known generally from the telephone number.[50] This would be a static and broad area such as a city within an area code.[51] In contrast, the antenna location information would demonstrate movement of the telephone and implicitly of the caller.[52] The FCC responded that even with POTS, law enforcement could know the exact location of a tapped telephone by using emergency services databases or telephone company records.[53] Therefore, knowing that a caller is within range of a particular cellular tower would actually provide less specific location information than that obtainable with POTS.[54]

Second, the CDT argued that CALEA's "origin" and "destination" terminology could not support location information as both terms have

---

45. *Id.*

46. *Id.*

47. *See infra* text accompanying notes 48-66.

48. *U.S. Telecom Ass'n*, 227 F.3d at 455.

49. *Id.*

50. *Id.* at 458 (quoting section 103(a)(2) of CALEA, codified at 47 U.S.C. § 1002(a)(2) (1994)). "[C]all-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)." 47 U.S.C. § 1002(a)(2). A "pen register" is a record of outgoing telephone numbers dialed from a particular telephone. 18 U.S.C. § 3127(3) (1994). A "trap and trace device [is] a device . . . which captures the incoming electronic or other impulses which identify the originating number" of an instrument or device from which a wire or electronic communication was transmitted. *Id* § 3127(4).

51. *U.S. Telecom Ass'n*, 227 F.3d at 458.

52. *Id.*

53. *Third Report*, ¶ 39, 14 F.C.C.R. 16,794, 16,813 (1999). US West commented that while the exact physical location of a wired telephone can be obtained from its number, that information is "incidental and should not be read as an underlying mandate of CALEA." *Id.* ¶ 41, 14 F.C.C.R. at 16,814.

54. *Id.* ¶ 39, 14 F.C.C.R. at 16,813.

"obvious meanings apart from location."[55] Presumably, the CDT believed that origin "obviously" meant the telephone number of the caller and destination "obviously" meant the telephone number called.[56] Interpreting the terms to mean a cellular antenna site as well as the "obvious meanings" violated the canon of statutory construction that each word of a statute has a single and unique meaning.[57] The FCC responded that CALEA defined call-identification information as both "dialing" and "signaling" information.[58] According to the FCC, CALEA's description of call-identification information as "dialing" information meant that things like telephone numbers were call-identification information.[59] Further, according to the FCC, CALEA also defined call-identification information as "signaling" information, which included the signals between the antenna and the telephone.[60] Therefore, call-identification information, according to the FCC, included both telephone numbers and antenna location information.[61]

Finally, the CDT argued that, since a mobile phone is usually used by the subscriber, location information is more "personally revealing" than similar wireline information would be.[62] That is, the owner is the individual using the cellular telephone in almost every instance.[63] In contrast, numerous persons often use wired telephones.[64] Since a higher volume of use offers some anonymity, a public telephone, where anyone enters information, is a stark contrast to cellular telephones, in which information was likely entered by the owner of the telephone.[65] Therefore,

---

55. *Id.* The relevant text from CALEA states, "the term 'call-identifying information' means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunication carrier." 47 U.S.C. § 1001(2) (1994).

56. *Third Report*, ¶ 39, 14 F.C.C.R. at 16,813. The J-Standard defined "origin" and "destination" as the telephone number of the caller and recipient respectively. *U.S. Telecom Ass'n*, 227 F.3d at 459.

57. *Third Report*, ¶ 39, 14 F.C.C.R. at 16,813. Canons of construction are like Newtonian physics in that for every canon there is an equal and opposite canon. Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes are to be Construed*, 3 VAND. L. REV. 395, 401-06 (1949-1950). Here the FCC offset the "unique meaning" canon with a canon stating that statutory language cannot be reduced to "mere surplusage." *Third Report.*, ¶ 44, 14 F.C.C.R. at 16,815 & n.95. The FCC reasoned that if the terms "origin" and "destination" had meaning only in the context of "dialing" information, the term "signaling" information would be reduced to "mere surplusage." *Id.*

58. *Third Report*, ¶ 44, 14 F.C.C.R. at 16,815.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.* ¶ 39, 14 F.C.C.R. at 16,813.

63. *Id.*

64. *Id.*

65. *Id.*

monitoring a cellular telephone reveals more about the caller than monitoring a wired telephone because there is no anonymity.[66]

The CDT also attacked the J-Standard's inclusion of packet-mode data.[67] According to the CDT, the data separation difficulties with packet-mode data would necessarily allow law enforcement access to call content even when it had satisfied only the lesser legal standards for obtaining call identifying information via a pen register or a trap and trace device.[68] The FCC took note that packet-mode data implicated privacy concerns because of the data separation difficulties.[69] The FCC, however, decided that the issue was not ripe for decision because further study of the technology was needed.[70] The FCC asked the telecommunications industry to study the problem and find a solution; however, the FCC tentatively let the requirement stand.[71]

After rejecting the CDT petition regarding antenna location and packet-mode data, the FCC adopted four of the custom calling features requested by the FBI.[72] These included the capability to capture digits after a call is connected, or "post-cut-through dialed digit extraction."[73] A second capability provided signals indicating that a party to a conference call is on hold, joining the conversation or hanging up.[74] The third item provided electronic signals indicating the subject is forwarding calls to another telephone or switching to a waiting call.[75] The fourth item notified law enforcement when the marked telephone received a network message, such as a telephone ring, busy signal, call waiting indication, or a message.[76] Given an adverse FCC decision, Petitioners sought judicial review.[77]

---

66. *Id.*

67. *Further Notice*, ¶ 59, 13 F.C.C.R. 22,632, 22,660 (1998).

68. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 456 (D.C. Cir. 2000). There are differing legal standards for different kinds of wiretaps. *Compare* 18 U.S.C. § 2518(2) & (3) (1994) (obtaining call content requires law enforcement to show probable cause of a serious crime, as defined by the statute and to obtain a judicial warrant) *with* 18 U.S.C. § 3122(b)(2) (1994) (obtaining records of incoming and outgoing telephone numbers requires only a certification by law enforcement that "the information likely to be obtained is relevant to an ongoing criminal investigation").

69. *Third Report*, ¶¶ 55-56, 14 F.C.C.R. 16,794, 16,819-20 (1999).

70. *Id.*

71. *Id.*

72. *U.S. Telecom Ass'n*, 227 F.3d at 456. The FCC adopted four capabilities in whole, two in part, and rejected three. *Id.* Only the four provisions adopted in whole were later challenged by the Petitioners. *Id.*

73. *Third Report*, ¶¶ 112 & 123 at 16,842, 16,846.

74. *Id.* ¶¶ 68, 74-75 at 16,825, 17,827-28.

75. *Id.* ¶¶ 76 & 82 at 16,828, 16,829-30.

76. *Id.* ¶¶ 83 & 89 at 16,832-33.

77. *U.S. Telecom Ass'n*, 227 F.3d at 456-57. Petitioners included: The United States Telecom Association, the Cellular Telecommunications Industry Association, the Center for

Petitioners argued generally that the FCC exceeded its statutory authority and ignored CALEA's privacy and funding requirements.[78] The FBI and the Department of Justice filed a brief in support of the FCC decision.[79] The Circuit Court of Appeals for the District of Columbia *held* that the FCC implementation order regarding cellular tower locations and packet-mode data was proper, but that the order regarding inclusion of the custom calling features was improper.[80]

II. LEGAL BACKGROUND

Telephone wiretaps are a form of eavesdropping, which has long been a tort.[81] Today, wiretaps constitute a search and seizure of communications.[82] Moreover, wiretaps may constitute an indiscriminate dragnet, catching innocent third persons in the search.[83] Therefore, telephone wiretaps implicate the Fourth Amendment, which states:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[84]

Several Supreme Court cases have interpreted what wiretaps are "reasonable" within the meaning of the Fourth Amendment.[85] Additionally,

---

Democracy and Technology, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the American Civil Liberties Union. *Id.* The following groups petitioned for a removal of the dialed digit extraction capability: the Telecommunications Industry Association, the Personal Communications Industry Association, Sprint PCS, and U.S. West. *Id.* at 457.

78. *Id.*

79. *Id.*

80. *Id.* at 463-65.

81. Berger v. New York, 388 U.S. 41, 45 (1967). At common law, the eavesdropper stood under the eaves of a house in order to listen to the conversation inside. *Id.*

82. Katz v. United States, 389 U.S. 347, 353 (1967).

83. *Berger*, 388 U.S. at 65 (Douglas, J., concurring).

> Thus in [United States v. Coplon, 91 F. Supp. 867 (D. D.C. 1950), *rev'd* 191 F.2d 749 (D.C. Cir. 1951)] wiretaps of the defendant's home and office telephones recorded conversations between the defendant and her mother, a quarrel between a husband and wife who had no connection with the case, and conferences between the defendant and her attorney concerning the preparation of briefs, testimony of government witnesses, selection of jurors and trial strategy.

Id.

84. U.S. CONST. amend. IV.

85. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 466 (1928) (finding a wiretap did not violate the Fourth Amendment when there was no entry onto the defendant's property); *Katz*, 389 U.S. 347, 353-54 (determining that a trespass standard for Fourth Amendment protection is too

Congress has enacted communication statutes that affect the permissible scope, method, and means of wiretaps.[86]

A. WIRETAP LAW IN THE EARLY YEARS, 1876-1934

Although the telephone was patented in 1876, there was little regulation of the medium, especially on a federal level, until into the 1930s.[87] Despite the extensive use of the telegraph in the nineteenth century, no dedicated federal agency existed to regulate communications carriers until 1934.[88] It was not until 1928 that the Supreme Court considered whether the Fourth Amendment protects telephonic communication.[89]

In *Olmstead v. United States*,[90] the United States Supreme Court first decided whether a wiretap is a search and seizure under the Fourth Amendment.[91] It ruled that wiretaps did not constitute either a search or a seizure under the Fourth Amendment.[92] In *Olmstead*, federal agents tapped the copper telephone lines outside the office of Olmstead who, the agents suspected, was violating prohibition laws.[93] The agents never entered Olmstead's office nor did the agents seize any tangible thing from Olmstead.[94]

---

narrow); Smith v. Maryland, 442 U.S. 735, 745-56 (1979) (finding no Fourth Amendment protections exist for telephonic data willingly provided to third parties).

86. *See, e.g.* Communications Act of 1934, Pub. L. No. 73-415, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.); Title III to the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211 (codified as amended in scattered sections of 18 U.S.C.); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended in scattered sections of 18 & 47 U.S.C.).

87. Pub. L. No. 75-415, 48 Stat. 1064 (1934) (codified as amended in scattered sections of 47 U.S.C.) On the other hand, the states were relatively active in providing statutory protection against electronic eavesdropping. *See infra* note 93; *see also Berger*, 388 U.S. at 45-46. For example, California made interception of telegraph, and later telephone, communications illegal as early as 1862. *Id.*

88. Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified as amended at 47 U.S.C. § 151 (1994 & Supp. V 1999)).

89. *Olmstead*, 277 U.S. at 455.

90. 277 U.S. 438 (1928).

91. *Olmstead*, 277 U.S. at 455.

92. *Id.* at 466.

93. *Id.* at 455-56. Wiretapping was a misdemeanor under applicable Washington State law. *Id.* at 466. To that end, Chief Justice Taft stated, for the Court, "[a] standard which would forbid the reception of evidence if obtained by other than nice ethical conduct by government officials would make society suffer and give the criminals greater immunity than has been known heretofore." *Id.* at 468. In response, Justice Holmes rendered an oft-quoted remark, "I think it is a less evil that some criminals should escape than that Government should play an ignoble part [in illegal activity]." *Id.* at 470. Washington State was not alone; in 1928, twenty-five states, including North Dakota and South Dakota, made wiretapping a criminal offense. *Id.* at 479 & n.13 (Brandeis, J., dissenting). Minnesota, North Dakota, South Dakota and thirty-two other states prohibited telecommunication carriers from assisting law enforcement in a wiretap. *Id.*

94. *Id.* at 457, 466.

The Court determined that without a physical intrusion there could be no search within the meaning of the Fourth Amendment's "houses, papers and effects" language.[95]

There was no search because the *Olmstead* Court read into the Fourth Amendment a "physical invasion" standard.[96] That is, to constitute a search there must first be some invasion, or trespass, upon the property of the complainant.[97] The only property the agents in *Olmstead* ever physically touched was that of the telephone company, not that of the complainant.[98] Since there was no intrusion, there was no search.[99] Hence, the Court concluded, the mere recording of the electronic signals constituting Olmstead's voice from copper wires lying outside his property was not a search because there was no entry onto his property.[100]

The *Olmstead* Court next determined whether there had been a Fourth Amendment seizure.[101] Consistent with its search analysis, the Court determined that since the electronic data was not tangible, it was not capable of Fourth Amendment seizure.[102] Electronic data was not, strictly construed, a "house," "paper," or "effect" within the meaning of the Fourth Amendment.[103] Nothing about the electrons that constituted Olmstead's telephonic messages was tangible, and therefore the messages were not "effects."[104] Therefore, the electronic capture of Olmstead's voice did not constitute a seizure within the Court's understanding of the Fourth Amendment.[105]

In his dissent, Justice Brandeis warned of a danger in strictly construing the language of a 1791 amendment when applying its principles to technological searches and seizures in 1928.[106] To Justice Brandeis, the Court's requirement that something be tangible to receive Fourth Amendment protection was too narrow.[107] Evolving technology threatened to

95. *Id.* at 457 (quoting U.S. CONST. amend. IV).
96. *Id.* at 456.
97. *Id.*
98. *Id.* at 457.
99. *Id.* at 456.
100. *Id.* at 466.
101. *Id.*
102. *Id.*
103. *Id.* (citing U.S. CONST. amend. IV).
104. *Id.*
105. *Id.*
106. *Id.* at 472 (Brandeis, J., dissenting). "Legislation, both statutory and constitutional is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions. . ." *Id.* (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).
107. *Id.*

increase the sting of government surveillance unless constitutional interpretation kept pace because technology was transforming once tangible things, like communications, into mere patterns of electrons.[108] While the social function of communication had not changed, the Court afforded communications less protection because of an accident of technology.[109] Justice Brandeis found no comfort in the fact that such surveillance was used for the purportedly benign purpose of catching criminals because, to Justice Brandeis, the wiretap was a tool of tyranny.[110]

B. WIRETAP LAW FOR A DEVELOPED TECHNOLOGY, 1934-1984

In 1934, Congress reacted to *Olmstead* with the Communications Act.[111] In addition to creating the FCC, the Communications Act made surveillance without consent of the caller a violation of federal law.[112] The

---

108. *Id.* at 474.

> Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> . . . The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

Id. at 473-74. Some commentators have noted the similarity of this prediction to Internet and e-mail surveillance technologies, where state or private actors can, theoretically, enter and copy a wired hard drive under the cloak of secrecy and without any physical intrusion. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 38-39, 59 (2000); *see also Hearing on the Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age, Before the Senate Judiciary Comm.*, 106th Cong. (2000) (statement of Senator Patrick Leahy, Ranking Member).

> The means by which law enforcement authorities may gain access to a person's private effects is no longer limited by physical proximity, as it was in the time of the Framers. New communications methods and surveillance devices have dramatically expanded the opportunities for surreptitious law enforcement access to private messages and records from remote locations.

Id.

109. Olmstead v. United States, 277 U.S. 438, 474 (1928).

110. *Id.* at 479.

> [I]t is also immaterial that the intrusion was in the aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. . . . The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.

Id. "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping." *Id.* at 476.

111. Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified as amended in scattered sections of 47 U.S.C.) (providing the first federal privacy protections for telephonic communications); *see also* Berger v. New York, 338 U.S. 41, 51 (1967) (noting the belief that the Communications Act was a response to *Olmstead*).

112. 47 U.S.C. §§ 151 & 605 (1994 & Supp. V 1999).

Communications Act, therefore, offered electronic communication statutory protection against surveillance despite *Olmstead*'s denial of similar constitutional protections.[113] Therefore, electronic surveillance was constitutionally permissible but illegal under federal statutes.[114] Two subsequent Supreme Court decisions found a middle ground in which law enforcement could collect telephonic recordings via a wiretap, although the Communications Act excluded the recorded information from use as evidence at trial.[115] Subsequent changes in the law, constitutional and statutory, would end the uneasy state of affairs created by the juxtaposition of *Olmstead* and the Communications Act.[116]

1. *Evolving Constitutional Standards*

The Supreme Court returned to the wiretap issue twice in 1967.[117] First, the Court considered *Berger v. United States*.[118] The issue was whether a New York statute allowing telephonic wiretaps when there was "reasonable ground" to believe evidence of a crime could be obtained was permissible under the Fourth, Fifth, Ninth, and Fourteenth Amendments to the Constitution.[119] Justice Clark, writing for the Court, concluded that the statute allowed invasions into a "constitutionally protected area."[120] Further, since the New York statute only required a "reasonable ground," it did not satisfy the particularity requirement of the Fourth Amendment.[121] Thus, the statute resembled an impermissible general warrant.[122] The Court found the New York statute unconstitutional for lack of a particularity require-

---

113. *Compare Olmstead*, 277 U.S. at 466 *with* 47 U.S.C. § 605.

114. *Compare Olmstead*, 277 U.S. at 466 *with* 47 U.S.C. § 605.

115. BeVier, *supra* note 1, at 1065-66 (citing Nardone v. United States, 302 U.S. 379, 382 (1937)); *see also* Nardone v. United States, 308 U.S. 338, 341 (1939).

116. *See infra* text accompanying notes 117-148.

117. Berger v. New York, 388 U.S. 41, 43 (1967); Katz v. United States, 389 U.S. 347, 349 (1967).

118. 388 U.S. 41 (1967).

119. *Berger*, 388 U.S. at 43 n.1.

120. *Id.* at 43. Justice Clark referred to *Wong Sun v. United States*, 371 U.S. 471 (1963) (considering the scope of the exclusionary rule) to support his assertion that wiretapping is Fourth Amendment activity because the Fourth Amendment "protect[s] against the overhearing of verbal statements." *Id.* at 52.

121. *Id.* at 55-56.

122. *Id.* at 58. The Court stated:

> New York's broadside authorization rather than being "carefully circumscribed" so as to prevent unauthorized invasions of privacy actually permits general searches by electronic devices, the truly offensive character of which was first condemned in *Entick v. Carrington*, 19 How. St. Tr. 1029 [(1765)], and which were then known as "general warrants." The use of the latter was a motivating factor behind the Declaration of Independence.

Id.

ment; however, it fell to the concurring opinion of Justice Douglas to suggest that *Olmstead* was therefore overruled and that wiretapping constituted a Fourth Amendment activity.[123]

Whether electronic eavesdropping was, in fact, Fourth Amendment activity was at issue in *Katz v. United States*.[124] In *Katz*, federal agents had attached a concealed microphone to the outside of a public telephone booth that they suspected Katz would use.[125] He did, and the federal agents used the recorded communication to arrest Katz.[126] The issue was whether the secret recording violated Katz's Fourth Amendment expectation of privacy.[127]

The Court found that law enforcement had violated the Fourth Amendment by bugging the public telephone line used by Katz.[128] Justice Harlan's concurring opinion reasoned that the Fourth Amendment provides a "reasonable expectation of privacy" to individuals.[129] Harlan then outlined the now controlling test for implicating the Fourth Amendment: whether an individual has a subjective expectation of privacy in a particular action and whether society is willing to accept that expectation as reasonable.[130] Since Katz took steps to ensure his privacy, such as shutting the door to the booth, he subjectively expected privacy.[131] Furthermore, Harlan reasoned that Katz's expectation was objectively reasonable because people expect privacy when they shut a door to the world.[132] Since Katz had a reasonable expectation of privacy, the Fourth Amendment applied.[133] Therefore, the federal agents should have obtained a warrant before placing the microphone on the booth.[134]

Justice Stewart, writing for the *Katz* Court, referred to the *Olmstead* decision as entertaining a "narrow view" of the meaning of the Fourth Amendment.[135] The Court commented, "the Fourth Amendment protects people, not places. What [a person] seeks to preserve as private, even in an

123. *Id.* at 64 (Douglas, J., concurring).
124. 389 U.S. 347 (1967).
125. *Katz*, 389 U.S. at 348.
126. *Id.*
127. *Id.* at 349.
128. *Id.* at 348, 359.
129. *Id.* at 361 (Harlan, J., concurring).
130. *Id.*
131. *Id.*
132. *Id.* The Court made no mention of third parties who may have used that same booth that day. *Id.*
133. *Id.*
134. *Id.*
135. *Id.* at 353.

area accessible to the public, may be constitutionally protected."[136] Hence, the Court abandoned *Olmstead* insofar as it required a trespass before state action constituted a search.[137] Further, the Court overturned *Olmstead*'s protection against a seizure of only tangible things.[138] The Court found that the Fourth Amendment protects not only tangible things, but also the "recording of oral statements."[139] Therefore, the Fourth Amendment permits telephonic searches and seizures only if law enforcement first obtains a judicial warrant based upon probable cause.[140]

2. *Congressional Reaction*

Congress codified the *Katz* warrant requirement in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).[141] Any telephonic information that is call content, as opposed to call-identifying information, is subject to the Title III warrant requirement.[142] Title III sets out several requirements that had to be satisfied before a magistrate issued a wiretap warrant.[143] For example, every application for a warrant must be in

---

136. *Id.* at 351. However, searches of "open fields," do not implicate Fourth Amendment protections. Oliver v. United States, 466 U.S. 170, 184 (1984). "Open fields" is a term of art as it refers to anything outside the curtilage of a dwelling and thus need not be either "open" nor a "field." *Id.* at 180 & n.11. The Court reasoned that real property is not an "effect" within the meaning of the Fourth Amendment, and even if it were, there can be no reasonable expectation of privacy outside protected curtilage. *Id.* at 176, 178-79. The *Oliver* dissent pointed out that the actions of Katz in the telephone booth were outside any kind of protected curtilage yet protected by a reasonable expectation of privacy. *Id.* at 185. Nevertheless, despite this apparent contradiction the Court made no effort to overrule *Katz*. *Id.* Hence both *Katz* and *Oliver* stand as good law although their co-existence can, at times, be uneasy. *Id.*

137. Katz v. United States, 389 U.S. 347, 351 (1967).

138. *Id.* at 353.

139. *Id.*

140. *Id.* at 356.

141. Wiretapping and Electronic Surveillance Act (Title III), Pub. L. No. 90-351, 82 Stat. 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (1994)).

142. United States v. New York Telephone Co., 434 U.S. 159, 166-67 (1977).

143. 18 U.S.C. § 2518(1) reads in part:

> Each application . . . shall be made in writing. . . . Each application shall include:
>
> a. the identity of the . . . officer making the application;
>
> b. a full and complete statement of the facts and circumstances relied upon by the applicant, . . . a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, . . . a particular description of the type of communications sought to be intercepted, . . . the identity of the person . . . whose communications are to be intercepted;
>
> c. a full and complete statement as to whether or not other investigative procedures have been tried and failed;
>
> d. a statement of the period of time for which the interception is required to be maintained;
>
> e. . . . all previous applications known to the individual authorizing and making the application;

writing and affirmed by oath.[144] The application must contain the identity of the investigating officer.[145] The application must list all facts and circumstances justifying the need for a wiretap and all the less evasive measures that have been tried and have failed, and why less evasive measures will likely not work in the future.[146] Finally, the applicant must identify when and for how long the wiretap will be in place as well as identifying any previous wiretap applications.[147] The combined effect of *Katz* and Title III is to extend Fourth Amendment protection to telephonic communication and amend the Communications Act to allow unauthorized wiretapping given a warrant.[148]

3. *Continued Evolution of Legal Standards*

Title III protections were broad and outlawed all forms of telephonic eavesdropping not otherwise authorized in the legislation.[149] However, in *Smith v. Maryland*[150] the Supreme Court narrowed the scope of protected electronic data.[151] The Fourth Amendment does not protect pen registers.[152] *Smith* relied on the reasonable expectation of privacy test first found in Justice Harlan's concurrence in *Katz*.[153] There is no reasonable expectation of privacy in something willingly given to another.[154] The Court determined that since the pen register was a recording of information willingly provided to third parties, namely telecommunication carriers, there was no expectation of privacy that society was prepared to accept as reasonable.[155] Without a reasonable expectation of privacy there is no search within the

---

f. where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception.

Id.

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.*

148. *Compare* Katz v. United States, 389 U.S. 347, 359 (1967) (extending Fourth Amendment protection to records of telephonic communications) *with* 18 U.S.C. § 2518 (allowing unauthorized electronic monitoring of telephonic communication given a warrant).

149. BeVier, *supra* note 1, at 1068. It has been argued that Title III wiretapping protections have eroded. ROSEN, *supra* note 108, at 37. Wiretaps were originally allowed only for crimes involving violence or national security (e.g., treason and espionage). *Id.* However, by 1996, seventy-one percent of all wiretaps involved drug cases. *Id.*

150. 442 U.S. 735 (1979).

151. *Smith*, 442 U.S. at 742 (regarding pen registers).

152. *Id.*; *see also* 18 U.S.C. § 3127(3) (1994) (defining pen register).

153. *Smith*, 442 U.S. at 740 (citing *Katz*, 329 U.S. at 361 (Harlan, J., concurring)).

154. *Id.* (citing *Katz*, 329 U.S. at 351).

155. *Id.* at 742.

meaning of the Fourth Amendment.[156] A warrant is not, therefore, required to obtain pen registers.[157]

In 1986, Congress extended limited statutory protection to pen registers in the Electronic Communications Privacy Act (ECPA).[158] To monitor pen registers and trap and trace devices under ECPA, law enforcement must merely certify that "the information likely to be obtained is relevant to an ongoing criminal investigation."[159] This limited protection has led some to criticize the ECPA as insufficient.[160] According to Senator Patrick Leahy, the law currently requires federal judges to automatically grant prosecutor requests for pen registers or trap and trace orders.[161] While limited, the ECPA protection for pen registers is a step beyond *Smith*, which denied pen registers as well as trap and trace devices Fourth Amendment protections.[162]

The guiding principles of telecommunications law going into the digital era were these: (1) *Katz* and Title III require a warrant in order to collect call content via a wiretap; and (2) while *Smith* denied pen registers Fourth Amendment protection, the ECPA requires that a law enforcement official seeking pen register information certify that the information is relevant to an ongoing investigation.[163] The protection afforded to pen registers as well as trap and trace devices is limited.[164] The next challenge would be to apply these principles to the rapidly developing technologies of the digital era.[165]

C. WIRETAP LAW IN THE DIGITAL ERA, 1984-2001

While federal constitutional and statutory law limited law enforcement's ability to monitor digital telecommunications, the technology itself came to act as a barrier to government surveillance.[166] The replacement of copper telephone lines with fiber optics, the introduction of computerized switching, as well as the plethora of new communication technologies developed after the 1984 breakup of AT&T stood as barriers to law enforce-

156. *Katz*, 389 U.S. at 361.

157. *Smith*, 442 U.S. at 742.

158. 18 U.S.C. § 3127 (1994).

159. 18 U.S.C. § 3122(b)(2) (1994). Trap and trace devices are records of incoming telephone numbers; for example, caller-id is a trap and trace device. *Id.* § 3127(4).

160. Leahy, *supra* note 108. Leahy describes the limited judicial protection as a mere "rubber stamp." *Id.*

161. *Id.*

162. *Compare* 18 U.S.C. § 3122 *with Smith*, 442 U.S. at 742.

163. *See supra* text accompanying notes 148 and 159.

164. 18 U.S.C. § 3122(b)(2).

165. *See infra* text accompanying notes 166-92.

166. BeVier, *supra* note 1, at 1050.

ment's wiretapping efforts.[167] Law enforcement agencies argued that they needed the telecommunications industry's assistance to preserve law enforcement's ability to conduct electronic surveillance.[168] In response, the 103d Congress passed CALEA.[169]

CALEA mandates that the telecommunications industry make its digital systems technologically capable of assisting law enforcement interception and monitoring of individual telephone calls as well as obtaining call-identifying information.[170] Call-identification information is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility or service of a telecommunications carrier."[171] CALEA requires that call-identification information be "reasonably available" to the telecommunications carrier before being included in implementation standards.[172] "Reasonably available" information is defined as that which is present at a carrier's "intercept access point" (IAP).[173]

Congress intended that CALEA preserve the status quo regarding surveillance capabilities.[174] In other words, law enforcement should not have access to more personal information due to an accident of technology.[175] The information available to law enforcement from CALEA affected tech-

---

167. *Further Notice*, ¶ 3, 13 F.C.C.R. 22,632, 22,635 (1998); *see also* Rosow, *supra* note 10, at 1058; BeVier, *supra* note 1, at 1050. According to BeVier:

> The break up of the AT&T . . . in 1984 unleashed a burst of technological progress and entrepreneurial activity in telecommunications. These developments, in tandem with the pace of progress in the computer industry and the remarkably swift emergence of the Internet as a mainstream tool of commerce, information dissemination, and all manner of human conversation, have triggered a communications revolution whose scope and magnitude could not possibly have been foreseen.

Id.

168. Hildegard A. Senseney, Note, *Interpreting the Communications Assistance for Law Enforcement Act of 1994: The Justice Department Verses the Telecommunications Industry and Privacy Advocates*, 20 HASTINGS COMM. & ENT. L.J. 665, 668 (1998).

169. BeVier, *supra* note 1, at 1051. The first attempts at a surveillance of digital telephony bill were included in a 1991 anti-terrorism bill, sponsored by Senator Joseph Biden; the matter never made it to the Senate floor. *Id.* at 1071. After some efforts by the elder Bush Administration, the issue was handed off to the Clinton Administration. *Id.* Clinton-appointed FBI Director, Louis Freeh, finally mustered enough political influence to push a digital telephony bill (CALEA) through the Congress. *Id.* at 1075.

170. 47 U.S.C. §§ 1001 & 1002(a) (1994 & Supp. V 1999).

171. *Id.* § 1001(2).

172. *Id.* § 1002(a)(2).

173. *Third Report*, ¶ 28, 14 F.C.C.R. 16,794, 16,808 (1999). The IAP is the systemic point at which data is obtained by the telecommunication carrier. *Id.* ¶ 14, 14 F.C.C.R. at 16,803. The IAP is analogous to a water faucet where the faucet is the systemic point in a pipeline where water can be removed from the system and examined. *Id.*

174. H.R. REP. No. 103-827, at 22 (1994).

175. *Id.*

nologies is to be roughly equivalent to that obtained from traditional telephonic surveillance technologies.[176]

Congress directed the telecommunications industry to define what technologies would be necessary for implementing CALEA in order to promote uniform and efficient implementation.[177] Under CALEA, the telecommunications industry is to consult with law enforcement agencies, regulators, and consumers regarding implementation standards.[178] Although consulted, law enforcement agencies and personnel are not to dictate the specific design of communications equipment, services or features.[179] If other persons or agencies believe the industry standards are "deficient," they may petition the FCC for review.[180]

The FCC is only to change the industry standards after identifying a deficiency.[181] In identifying a deficiency, CALEA requires the FCC to consider five factors.[182] First, the implementation rules are to "meet the assistance capability requirements . . . by cost-effective methods."[183] Second, the rules must "protect the privacy and security of communications not authorized to be intercepted."[184] Third, the FCC should minimize the cost of implementation passed onto residential ratepayers.[185] Fourth, implementation standards must recognize that the public policy of the United States favors encouraging development and dissemination of new technologies and services to the public.[186] Finally, the implementation rules should provide telecommunications carriers with a reasonable amount of time for transition.[187]

Congress included a safe harbor provision for telecommunications equipment in use before January 1, 1995.[188] A telecommunications carrier may petition the FCC for a compliance analysis if the carrier believes it is not reasonable to make the carrier's pre-1995 equipment compliant.[189] If

176. *Id.*
177. 47 U.S.C. §§ 1002(b)(1) & 1006 (a)(1) (1994 & Supp. V 1999).
178. *Id.* § 1006(a)(1).
179. *Id.* § 1002(b)(1).
180. *Id.* § 1006(b).
181. *Id.*
182. *Id.*
183. *Id.* § 1006(b)(1).
184. *Id.* § 1006(b)(2).
185. *Id.* § 1006(b)(3). The Cellular Telecommunications Industry Association estimated that compliance cost for the core J-Standard would reach as high as $4 billion. *Third Report*, ¶ 20, 14 F.C.C.R 16,794, 16,805 (1999).
186. 47 U.S.C. § 1006(b)(4).
187. *Id.* § 1006(b)(5).
188. 47 U.S.C. § 1008(a) (1994); *see also Third Report*, ¶ 33, 14 F.C.C.R. at 16,810.
189. 47 U.S.C. § 1008(b)(1).

the FCC then finds that compliance is not reasonably achievable, the telecommunications carrier may ask the Attorney General to provide federal funding for the reasonable costs of compliance.[190] Whether or not the Attorney General allocates funds for an upgrade, the telecommunications carrier is considered CALEA compliant.[191] The federal government is to reimburse telecommunication carriers for equipment installed after January 1, 1995 for CALEA purposes.[192]

III. ANALYSIS

The court in *U.S. Telecom Ass'n v. FCC*[193] determined that CALEA did not support the addition of the custom calling capabilities desired by the FBI.[194] However, the court retained the antenna location and packet-mode data features that were originally included in the J-Standard.[195] Much of the *U.S. Telecom* opinion concerns the application of administrative law; that is, whether the FCC acted properly by reviewing the J-Standard when and as it did.[196] Underlying the administrative law matters, however, were concerns about privacy.[197] Congress directed the FCC and the telecommunications industry to consider privacy issues when implementing CALEA.[198] However, privacy is a broad and ambiguous term which is not defined in CALEA, and therefore the court needed to conceptualize what Congress meant by "privacy" in the context of each challenged capability.[199]

---

190. *Id.* § 1008(b)(2)(A). This money would be pulled from a congressional allocation for implementation expenses of $500 million for fiscal years 1995-1998. 47 U.S.C. § 1009 (1994).

191. *Id.* § 1008(d).

192. *Third Report*, ¶ 26, 14 F.C.C.R. at 16,807-08. This reimbursement is left to the discretion of the Attorney General. 47 U.S.C. § 1008(a).

193. 227 F.3d 450 (D.C. Cir. 2000).

194. *U.S. Telecom Ass'n*, 227 F.3d at 463. Judges Tatel, Ginsburg, and Randolph of the District of Columbia Circuit heard the *U.S. Telecom* case; Judge Tatel wrote the opinion. *Id.* at 453. The court heard the petitions of the CDT as well as the FBI; these petitions followed an FCC rulemaking. *Id.* at 455-57.

195. *Id.* at 464-65.

196. *Id.* at 457-60. Because the definition of call-identifying information was ambiguous, the court relied on *Chevron U.S.A., Inc. v. Natural Res. Def. Council*, 467 U.S. 837 (1984). *Id.* at 457. *Chevron* established a two-part test for interpreting agency interpretations of a statute. *Chevron*, 467 U.S. at 842-43. A court must determine whether Congress has spoken directly to the issue at hand, and if not, the agency interpretation must be based on a permissible construction of the language. *Id.*

197. *See U.S. Telecom Ass'n*, 227 F.3d at 459 (discussing the *Katz* reasonable expectation of privacy requirement).

198. 47 U.S.C. § 1006(b)(2) (1994).

199. *See U.S. Telecom Ass'n*, 227 F.3d at 463 (concerning the privacy implications of dialed digit extraction and whether retaining antenna location information was reasonable given privacy concerns) *and* at 464-65 (noting that packet-mode data has privacy implications that may have to

A. PACKET-MODE DATA

Whether packet-mode data would allow law enforcement greater access to information than tolerated by a particular warrant or pen register order was an issue in *U.S. Telecom.*[200] The court determined that the FCC decision to include packet-mode data in CALEA implementation standards was permissible.[201] Although the FCC recognized packet-mode data could provide too much private information to law enforcement, the FCC retained the capability.[202] The FCC did not turn a blind eye to the privacy problem; to deal with privacy concerns, the FCC requested that the telecommunications industry formulate a technological solution to the data separation problem.[203] In so doing, the FCC noted that its decision to implement the packet-mode requirement was merely an "interim" requirement.[204] The court sidestepped the issue of what legal standard is required to access data packets by stating that telecommunications carriers need not turn over the data unless law enforcement have "proper" legal authorization.[205]

The court did not decide what constitutes "proper" legal authorization.[206] Therefore, it remains unclear as to whether "proper" authorization means a wiretap warrant, a pen register subpoena, or something in the middle.[207] The court believed that it did not need to decide the issue because it was not squarely before the court and changing technology could act to make the problem moot.[208] Hence, the court skirted Fourth Amendment analysis by admitting to possible privacy concerns but remanding the

---

be re-visited). The primary source for defining "privacy" is the reasonable expectation of privacy test from *Katz*. Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring).

200. *U.S. Telecom Ass'n*, 227 F.3d at 465.

201. *Id.*

202. *Id.*

203. *Id.*

204. *Id.*

205. *Id.*

> CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization to obtain packets from which call content has not been stripped, nor may the Commission require carriers to provide the government with information that is "not authorized to be intercepted."

Id.

206. *Id.*

207. *Hearings on H.R. 5018, Electronic Communications Privacy Act of 2000, H.R. 4987, Digital Privacy Act of 2000, and H.R. 4908, Notice of Electronic Monitoring Act Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. (2000) (testimony of James X. Dempsey, Senior Staff Counsel for the Center of Democracy and Technology).

208. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 465 (D.C. Cir. 2000).

problem back to the telecommunications industry for a technological solution.[209]

B. ANTENNA LOCATION INFORMATION

Another issue was whether to retain antenna location information, as defined in the J-Standard.[210] The court emphasized that including antenna location information merely maintained a surveillance capability similar to that used in POTS.[211] Since the antenna is the medium through which the electronic message travels, it is the digital equivalent of copper wire.[212] Therefore, knowing the antenna location is like knowing the path or, at least, the general location of a tapped copper telephone wire.[213]

In retaining the antenna location requirement, the court faced the issue of whether call-identification information was limited to telephone numbers.[214] The FCC had answered this question in the negative by pointing to CALEA language defining call-identifying information as both "dialing" and "signaling" information where "signaling" information referred to the radio communication between the cellular telephone and the antenna.[215] In analyzing the same issue, the court relied on *Chevron U.S.A. v. Natural Resources Defense Counsel*.[216] *Chevron* tested agency interpretations of ambiguous statutory language.[217] According to the court, CALEA could have simply stated that call-identification information meant only telephone numbers if Congress had so intended.[218] Further, Congress did define call-

---

209. *Id.*

210. *Id.* at 462; *see also Third Report*, ¶ 44, 14 F.C.C.R. 16,794, 16,815 (1999).

211. *U.S. Telecom Ass'n*, 227 F.3d at 462.

212. *Id.*

213. *Id.* at 463-64. In response to this holding the Executive Director of the Electronic Privacy Information Center, Marc Rotenberg, stated, "[i]t is generally not the case that the law both provides law enforcement the right to conduct a search and also requires technical steps be taken prior to the issuance of a warrant to ensure that success in the search be assured." *Hearings on H.R. 5018, Electronic Communications Privacy Act of 2000, H.R. 4987, Digital Privacy Act of 2000, and H.R. 4908, Notice of Electronic Monitoring Act Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. (2000) (testimony of Marc Rotenberg, Executive Director Electronic Privacy Information Center).

214. *U.S. Telecom Ass'n*, 227 F.3d at 457.

215. *Third Report*, ¶ 44, 14 F.C.C.R. at 16,815.

216. 467 U.S. 837.

217. *Chevron*, 467 U.S. at 842-43.

218. *U.S. Telecom Ass'n*, 227 F.3d at 458. For this analysis the court relied on *Russello v. United States*, 464 U.S. 16 (1983). *Russello* states that "[w]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *Russello*, 464 U.S. at 23. Since Congress used the term "telephone number" elsewhere in CALEA but not in defining call-identifying information, the court assumed Congress intended the disparate exclusion. *U.S. Telecom Ass'n*, 227 F.3d at 458. Therefore, Congress must have meant call-identifying information to mean more than telephone numbers. *Id.*

identifying information as both dialing and signaling information, and therefore the definition should not be read narrowly as including only dialing information such as telephone numbers.[219] Hence, the court found that the FCC could interpret CALEA as including antenna location information under the *Chevron* standard.[220]

Finally, the court considered whether the antenna location requirement respected privacy concerns.[221] The J-Standard required more than a pen register order before law enforcement could access the information.[222] The Fourth Amendment does not protect a pen register because it is a record of information willingly provided to third parties.[223] However, location information is different; often it is not willingly provided to third parties and therefore more than a mere pen register is needed to access it.[224]

C. CUSTOM CALLING FEATURES

The court also determined whether the FCC erred in injecting custom calling features into the J-Standard.[225] The court found FCC inclusion of custom calling features to be an impermissible and arbitrary agency action.[226] For example, the FCC exceeded the bounds of the CALEA language by including the custom calling features.[227] To justify inclusion of the features, the FCC interpreted some CALEA provisions as having multiple definitions.[228] Namely, the FCC stated that the "origin" of a call meant not only the telephone number of an incoming call but also a call waiting tone, signals that a party was entering a conference call, and the release of a call from hold.[229] According to the court, the FCC never explained how

---

219. *U.S. Telecom Ass'n*, 227 F.3d at 458.

220. *Id.* The FCC was obligated to give effect to every portion of the statute according to the court. *Id.* at 463. Such is the rule of statutory construction from *Washington Market Co. v. Hoffman*, 101 U.S. 112 (1879). *Id.* at 462 (citing *Washington Market*, 101 U.S. at 115-16).

221. *Id.* at 464.

222. *Third Report*, ¶ 44, 14 F.C.C.R. 16,794, 16,815 (1999). How much more is not yet clear. *Cf. U.S. Telecom Ass'n*, 227 F.3d at 464 (making no comment on what the standard should be). However, even the Department of Justice agrees that more than a pen register is necessary; the Department said, "[a] pen register order does not by itself provide law enforcement with authority to obtain location information, and we have never contended otherwise." *Id.*

223. Smith v. Maryland, 442 U.S. 735, 742 (1979).

224. *U.S. Telecom Ass'n*, 227 F.3d at 464.

225. *Id.* at 460-63. The four custom calling features at issue were: dialed digit extraction, party hold/drop/join information, call forwarding and waiting information, and network messaging. *Id.* at 457.

226. *Id.* at 461 (referring to the excessive increased cost of including the capabilities that was not justified by the FCC).

227. *Id.* at 460.

228. *Id.*

229. *Id.* Additionally, the FCC used the term "termination" to mean the number of an outgoing call as well as signals indicating a call has been switched, held, or dropped. *Id.*

CALEA required these various interpretations of the language.[230] Without such an explanation, the court could not determine if the decision was the result of a reasoned decisionmaking process.[231]

The court was also concerned that the FCC failed to explain why any change of the industry's J-Standard was necessary.[232] CALEA required the FCC to make specific findings of deficiencies in the industry plan before the FCC could change it.[233] However, the FCC never noted any deficiencies in the J-Standard.[234] Additionally, the FCC failed to take proper notice of the increased cost of compliance when it added the FBI capabilities.[235] This was in contradiction to the CALEA mandate that the financial impact on industry and ratepayers be reasonable and minimal.[236]

However, the primary concern about the custom calling capabilities was the effect dialed digit extraction would have on the privacy of information not subject to the search.[237] Post-cut-through dialed digits can represent both call content and call identifying information.[238] For example, the

---

230. *Id.*

231. *Id.* In holding that the failure to explain amounted to a lack of reasoned decisionmaking, the court relied on *Motor Vehicles Mfrs. Ass'n v. State Farm Mut. Auto Ins. Co.*, 463 U.S. 29 (1983). The specific issue in *Motor Vehicle Mfrs.* was whether the Secretary of Transportation acted arbitrarily and capriciously in revoking passive restraint requirement from the motor vehicle safety standards. *Motor Vehicle Mfrs.*, 463 U.S. at 33. The Court required that there be a "rational connection between the facts found and the choice made." *Id.* at 43 (quoting Burlington Truck Lines, Inc. v. United States, 371 U.S. 156, 158 (1962)). Further, the agency must "explain why it has exercised its discretion in a given manner." *Id.* at 48. Only then will the choice be considered "the product of reasoned decisionmaking." *Id.* at 57.

232. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 460-61 (D.C. Cir. 2000).

233. 47 U.S.C. § 1006 (1994). "Were we to allow the Commission to modify the J-Standard without first identifying its deficiencies, we would weaken the major role Congress obviously expected industry to play in formulating CALEA standards." *U.S. Telecom Ass'n*, 227 F.3d at 461.

234. *U.S. Telecom Ass'n*, 227 F.3d at 460-61.

235. *Id.*

236. *Id.* The FCC knew compliance for the core J-Standard could reach $4 billion. *Id.* Despite this knowledge, the FCC included the four custom calling features, which increased compliance costs by forty-five percent. *Id.* The FCC never explained how adding to the already high costs of compliance was reasonable under CALEA. *Id.* To this the court responded that *Motor Vehicle Mfrs.* required the FCC to articulate an explanation for the action. *Id.* The explanation was to include "a rational connection between the facts found and the choice made." *Id.* (quoting *Motor Vehicle Mfrs.*, 463 U.S. at 43). Here the FCC never explained itself. *Id.*

237. *Id.* at 462.

238. *Id.* The court acknowledged that dialed digits can be either call identifying information or content. *Id.* The court provided the following examples:

> Some post-cut-through dialed digits are telephone numbers, such as when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. Post-cut-through dialed digits can also represent call content. For example, subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages. And when calling pharmacies to renew prescriptions, they enter prescription numbers.

digits are content when representing data such as a bank account number.[239] However, dialed digits are call identification information when representing a second telephone number.[240] Because dialed digits may constitute call content, a caller has a reasonable expectation of privacy in them.[241]

Since there is a privacy expectation in dialed digits, it might be argued that a Title III warrant is required for access because call content might be accessed.[242] However, the FCC asserted that dialed digits are obtainable with only a pen register.[243] According to the court, the FCC was obligated to explain how obtaining dialed digits with a pen register would comply with CALEA's privacy concerns.[244] Despite the need for such analysis, the FCC merely spoke of law enforcement's need for dialed digit information.[245] The court found that the utility of the capability is no substitute for a reasoned explanation as to why the information should be obtained with only the limited pen register protections.[246]

Further, the court noted, the FCC summarily rejected several alternative measures that would have addressed privacy concerns.[247] For example, the Personal Communications Industry Association recommended requiring a Title III warrant before extracting dialed digits.[248] Because these alternatives placed further burdens on law enforcement, the FCC rejected them.[249] At oral argument, counsel for the FCC stated, "we addressed ourselves to the privacy questions with a little bit of hand wringing and worrying."[250] The court responded, "[n]either hand wringing nor worrying can substitute for reasoned decisionmaking."[251] The FCC could not simply ignore the privacy implications inherent in a technological capability that can access call content with tools intended to capture only call identifying information.[252]

Id.

239. *Id.*

240. *Id.*

241. *Cf.* United States v. New York Tel. Co., 434 U.S. 159, 166-67 (1977) (stating that the Title III warrant requirement extends to the interception of any "contents" of a communication).

242. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000). "No court has yet considered that contention [that dialed digits may be obtained with a pen register] however, and it may be that a Title III warrant is required to receive all post-cut-through digits." *Id.*

243. *Id.*

244. *Id.*; *see also* 47 U.S.C. § 1006(b)(2) (1994).

245. *U.S. Telecom Ass'n*, 227 F.3d at 462.

246. *Id.*; *see also supra* text accompanying notes 158-62.

247. *Third Report*, ¶ 120, 14 F.C.C.R. 16,794, 16,845 (1999).

248. *Id.*

249. *U.S. Telecom Ass'n*, 227 F 3d. at 462.

250. *Id.* at 463.

251. *Id.*

252. *Id.*

In sum, the opinion denied the FBI requested custom calling capabilities, including dialed digit extraction, but retained the antenna location and packet-mode data provisions from the J-Standard.[253] Further, the court left open the possibility of returning to the packet-mode data issue in the future, as industry solutions are developed.[254]

IV. IMPACT

As a result of the decision in *U.S. Telecom*, many privacy questions will develop.[255] However, the effect of denying the FBI the capability to extract dialed digits is a major victory for privacy advocates because it assumes there is a reasonable expectation of privacy in dialed digits that are call content.[256] Another effect of this decision will be its impact on future lawmaking.[257] For example, the 106th Congress considered several reforms of federal communications law regarding cellular telephone location information.[258] In part, these reforms seek to fill the blanks left by CALEA, namely, the legal standard required to obtain location information from cellular communications.[259]

A third effect of *U.S. Telecom* will be its impact on developing digital technologies.[260] For example, *U.S. Telecom* requires communications carriers to make packet-mode data available to federal law enforcement.[261] Therefore, a precedent is set whereby industry may be required to assemble and make sense of digital messages for law enforcement.[262] This precedent is meaningful given that the Internet uses data packets to transmit information.[263] In the near future, there will be a debate as to whether Internet data-packets should be made available to LEAs, and this debate will need to consider the fact that, while technologically similar, Internet and telephonic

253. *Id.* at 463-65.

254. *Id.* at 465.

255. *See discussion infra* Part IV.A-B.

256. U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 462-63 (D.C. Cir. 2000).

257. *See infra* text accompanying notes 271-76. Between 1997 and 1999 Congress debated over 100 privacy focused bills and state governments looked at over 1000 measures. Toby Lester, *The Reinvention of Privacy*, THE ATLANTIC MONTHLY, March 2001, at 38.

258. H.R. 4908, 106th Cong. (2000); H.R. 4987, 106th Cong. (2000); H.R. 5018, 106th Cong. (2000).

259. Dempsey, *supra* note 207.

260. *See infra* text accompanying notes 277-90.

261. *U.S. Telecom Ass'n*, 227 F.3d at 465.

262. *Id.*

263. *See* Senseney, *supra* note 168, at 665 (stating that data packets are used on the Internet); *see also Further Notice*, ¶ 63, 13 F.C.C.R. 22,632, 22,661-62 (1998) (emphasizing that CALEA is to affect only telephony data packets and not those used for information services).

data-packets may carry with them starkly different expectations of privacy.[264]

A. NATIONAL IMPACT

The court denied law enforcement the dialed digit extraction capability and stole headlines in August of 2000.[265] By concentrating on privacy concerns, the court gave voice to a rising discontent within the American populace.[266] As technology has advanced during the twentieth century, the United States has become a less private place.[267] More and more Americans are concerned that "Big Brother" truly is watching.[268] This concern adversely affects a person's quality of life.[269] Denying a surveillance capability such as dialed digit extraction to law enforcement helps to ward off references to "Big Brother" by limiting the power of government to access private information.[270]

A second impact concerns the questions *U.S. Telecom* leaves open, namely the appropriate legal standards for obtaining location information.[271] *U.S. Telecom* stated that more than a pen register order is required to obtain location information.[272] Thus the baseline is established; however, still open is the question as to what more than a pen register is necessary.[273] During the 106th Congress, Representatives Bob Barr of Georgia and JoAnn Emerson of Missouri proposed the Digital Privacy Act

---

264. *The Fourth Amendment and the FBI's Carnivore Program, Before the Senate Judiciary Comm.*, 106th Cong. (2000) [hereinafter *Fourth Amendment*] (statement of Jeffrey Rosen, Associate Professor, George Washington University Law School).

265. John Schwartz, *Court Says FCC Gives FBI Too Much Wiretap Power*, THE WASHINGTON POST, Aug. 16, 2000, at E-1; Eric Lichtblau, *Privacy Advocates Win Ruling on Wireless Devices Communications*, L.A. TIMES, Aug. 16, 2000, at A4.

266. *Cf.* Lester, *supra note* 257, at 27 (stating that Americans are more concerned about privacy in the twenty-first century than they are about overpopulation, racial tensions, and global warming).

267. ROSEN, *supra* note 108, at 25 (referring to how recent changes in technology have helped to diminish privacy expectations once taken for granted).

268. *Cf.* Lichtblau, *supra* note 265 (referring to "Big Brother"); Lester, *supra* note 257 at 38 (noting the prevalence of "Big Brother" references). "Big Brother" is the fictional figurehead of the post-democratic state of Oceania in George Orwell's classic novel about a world without privacy and freedom. *See generally* GEORGE ORWELL, 1984 (1949).

269. ROSEN, *supra* note 108, at 19. According to Rosen, "[f]rom its earliest days, Jewish law recognized that it is the uncertainty about whether or not we are being observed that forces us to lead more constricted lives and inhibits us from speaking and acting freely in private places." *Id.*

270. *Cf.* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 462-63 (D.C. Cir. 2000) (denying the dialed digit capability to law enforcement and thus preventing "Big Brother" from "watching" the numerical content of a telephone call).

271. Dempsey, *supra* note 207.

272. *U.S. Telecom Ass'n*, 227 F.3d at 464.

273. Dempsey, *supra* note 207.

of 2000 as a partial solution to the problem.[274] Their Digital Privacy Act would require a judicial warrant based on probable cause before law enforcement could engage in tracking cellular telephones, as they move from cellular site to site.[275] Normally the warrant could only be issued if the suspect is thought to have committed or is committing a felony; however, the Digital Privacy Act would also allow tracking of cellular telephones without a warrant given the caller's permission.[276]

A third impact concerns whether, in the future, Internet service providers (ISPs) will be subjected to CALEA-like assistance requirements for Internet data packets.[277] CALEA does not apply to information technologies such as the Internet and e-mail.[278] While the ECPA allows searches of Internet and e-mail communications, CALEA does not require ISP assistance in conducting the search and seizure.[279] Therefore, there is a gap between telecommunications carriers and ISPs.[280]

The FBI sought to jump the gap by creating a program called "Carnivore."[281] Carnivore searches through the e-mail channeled through an ISP, looking for messages that fit search criteria entered by a programmer.[282] In the summer of 2000, the FBI issued a Carnivore disclosure with the expressed purpose of obtaining CALEA wiretap assistance from ISPs.[283] This

---

274. *See* H.R. 4987, 106th Cong. (2000) (resolving to enact six measures to increase digital privacy).

275. *Id.*

276. *Id.* There are numerous reasons why a person might consent to having his or her cellular telephone tracked; for example, tracking has helped to locate people caught in blizzards. Senseney, *supra* note 168, at 667.

277. *See infra* text and accompanying notes 278-85.

278. *See* 47 U.S.C. § 1002(b)(2)(A) (1994) (excluding information services from the CALEA assistance requirements); 47 U.S.C. § 1001(6) (1994) (defining information services). According to CALEA:

> The term "information services"—(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and (B) includes—(i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities; (ii) electronic publishing; and (iii) electronic messaging services.

Id. § 1001(6)(A) & (B).

279. *The Tenth Amendment and the Internet, Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. (2000) (attachment to testimony of Robert Corn-Revere, Attorney, Hogag & Hartson L.L.P.)

280. Leahy, *supra* note 108.

281. *Id.*; *see also* Carnivore Diagnostic Tool, *available at* http://www.fbi.gov.programs/carnivore/carnivore2.htm (last visited Aug. 27, 2000) [hereinafter Carnivore Diagnostic Tool].

282. *Internet and Data Interception Capabilities Developed by the FBI, Before the Subcomm. on the Constitution of the House Comm. On the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation).

283. Carnivore Diagnostic Tool, *supra* note 281.

is inconsistent with CALEA in that the assistance requirement does not apply to "information services," which are partially defined as "electronic messaging."[284] This apparent FBI misuse of CALEA may require judicial review; however, the events suggest that the FBI desires ISP assistance in tapping Internet-based communication.[285]

Any extension of wiretaps to the Internet and e-mail implicates an interesting issue: whether Internet or e-mail data packets enjoy the same expectation of privacy as telephonic data packets.[286] Some commentators have already weighed in; for example, Jeffrey Rosen, an associate professor of law at George Washington University Law School believes that obtaining Internet addressing information is far more invasive than telephone call identifying information.[287] A web address reveals content in ways that telephone numbers do not because the design of a web address often suggests something of the nature of the site.[288] Further, unlike an unrecorded telephone call, a LEA could log onto the Internet address obtained with a pen register and see the content of the communication.[289] Therefore, the issue is whether a mere pen register authorization is ever sufficient to access web addresses.[290]

---

284. 47 U.S.C. §§ 1002(b)(2)(A) & 1001(6) (1994).

285. Carnivore Diagnostic Tool, *supra* note 281.

286. *Fourth Amendment, supra* note 264 (testimony of Jeffrey Rosen).

287. *Id.*

> And yet the information revealed by Carnivore is far more invasive than the telephone numbers revealed by a pen register. The government has access to the identity of the recipient and sender of the specified communication, and, in the case of URL addresses, to the search terms that may have been entered in an Internet search. By reviewing the web sites a target has visited, the books he has skimmed, and the searches he has entered, law enforcement agents may have access to a granular picture of his interests and activities on line. In upholding the constitutionality of pen registers, the Supreme Court reasoned that citizens have no reasonable expectation of privacy in information, like telephone numbers, that they have voluntarily turned over to the phone company and that they expect the phone copy to record. But it is hardly clear that citizens feel similarly about records of their Internet searches and reading habits.

Id.

288. *Id.* For example, via a pen register, law enforcement could determine that a call to (701) 777-2941 went to the Law Review office at the University of North Dakota School of Law; but nothing of the call's content would be apparent from the number alone. *Cf. Id.* On the other hand, a LEA armed with a pen register would discover an Internet user visited http://www.law.und.nodak.edu/grades/; from this information, the LEA would know something of the content of the communication, that grades from the University of North Dakota School of Law were accessed. *Cf. Id.* Further, given current difficulties with data separation, if the data packet included the password to access the actual grades, an unscrupulous law enforcement agent could access even more communication content. *Cf. Id.*

289. *Cf. Id.* This will result in litigation asking whether viewing a web address obtained with a pen register is like a plain view observation and whether cyberspace is outside protected curtilage. *Cf.* Dempsey, *supra* note 207 (anticipating future litigation).

290. Dempsey, *supra* note 207.

B. NORTH DAKOTA IMPACT

Wiretaps in North Dakota are authorized by the *North Dakota Century Code*, and the requisite elements to obtain court authorization read much like the Title III requirements.[291] For example, the application must be in writing, based on probable cause, normal techniques must be tried, and all previous applications must be identified.[292] Further, telecommunication carriers are required to assist law enforcement in court-authorized wiretaps.[293] In North Dakota, the definition of communications subject to tapping already implicitly includes cellular technologies.[294] It follows, in these respects, the *U.S. Telecom* decision will not provide North Dakota law enforcement any capabilities beyond what they have under state law.[295]

However, North Dakota law, in another sense, may be inconsistent with CALEA.[296] North Dakota allows wiretapping of wire, electronic, or oral communications.[297] The statutory definition of electronic communica-

---

291. N.D. CENT. CODE § 29-29.2-02 (1991). The relevant portion of the statute reads:

> Each application for wiretapping or eavesdropping . . . must include:
>
> The identity of the law enforcement officer.
>
> A complete statement of the facts and circumstances . . . justify[ing] the belief that an order should be issued.
>
> A complete statement as to whether other investigative procedures have been tried and failed, or why they reasonably appear to be unlikely to succeed.
>
> A statement of the period of time for which the interception is required to be maintained.
>
> A complete statement of the facts concerning all previous applications.

Id. § 29-29.2-02(3).

292. *Id.*

293. N.D. CENT. CODE § 29-29.2-03 (1991). The North Dakota provision reads:

> An order authorizing the interception of a wire, electronic, or oral communication must, upon request of the applicant, direct that a communication common carrier shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that the carrier is according the person whose communications are to be intercepted. A communication common carrier furnishing these facilities or technical assistance must be compensated by the applicant for reasonable expenses incurred in providing the facilities or assistance.

Id.

294. *Compare* N.D. CENT. CODE § 29-29.2-03 (allowing interception of "electronic communication") *with* N.D. CENT. CODE § 29-29.2.-01(4) (1991) (defining "'[e]lectronic communication' [as a] transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system").

295. *Compare* 18 U.S.C. § 2518(1) (1994 & Supp. V 1999) (listing requirements for a Title III warrant to tap communication devices) *with* N.D. CENT. CODE § 29-29.2-02 (listing similar North Dakota requirements). *Compare* 47 U.S.C. § 1002 (1994 & Supp. V 1999) (requiring industry assistance) *with* N.D. CENT. CODE § 29-29.2-03 (requiring industry assistance).

296. *See infra* text accompanying notes 297-98.

297. N.D. CENT. CODE § 29-29.2-02. The statute refers to "wiretapping" and "eavesdropping;" however, these terms are not defined. *Id*; N.D. CENT. CODE § 29-29.2-01 (providing

tion implicitly includes cellular technologies; however, the statute excludes tracking devices.[298] Although the *U.S. Telecom* court did not consider antenna location information to be a tracking capability, Congress has considered allowing real-time tracking of cellular telephones, given a Title III warrant.[299] Therefore, two issues will develop in North Dakota law.[300] First, whether the definition of electronic communication excludes cellular telephones if they are used as tracking devices.[301] Second, whether cellular telephones can be wiretapped if excluded from the definition of electronic communication.[302] Legislative or judicial consideration will be required if the antenna location capability in CALEA or developing cellular technologies weigh in favor of defining cellular telephones as tracking devices.[303]

V. CONCLUSION

U.S. Telecom involved the first review of legislation dealing with wiretaps of digital telephone technology.[304] The court concluded that dialed digit extraction exacts too great a privacy cost, but that antenna location information as well as packet-mode data might be acceptable.[305] However, the court left the door open to future decisions regarding the requisite legal standard for obtaining antenna location information and packet-mode data.[306]

Notably, as a direct result of the September 11th attack, Congress is again looking at the wiretap law.[307] Like with CALEA in 1994, the Justice

---

definitions). The defined term most like "wiretapping" and "eavesdropping" is "intercept" which refers to wire, electronic, and oral communications. *Id.* § 29-29.2-01(6). Additionally, the statute authorizing "wiretapping" and "eavesdropping" uses the wire, electronic, and oral language elsewhere. *Id.* § 29-29.2-02(5)(d), (7), (9), (11), (12), (14)-(19). Therefore, the closest approximation, from the statutory language of what the legislature intended to be subject to wiretapping, is wire, electronic, and oral communications. *Id.* §§ 29-29.2-01 & 29-29.2-02.

298. *Id.* § 29-29.2-01(4).

299. H.R. 4987, 106th Cong. (2000).

300. *See supra* text accompanying notes 296-98.

301. *Compare* H.R. 4987, 106th Cong. (2000) (proposing limited use of cellular telephones as tracking devices) *with* N.D. CENT. CODE § 29-29.2-01 (excluding tracking devices from the definition of electronic communication).

302. *See* N.D. CENT. CODE § 29-29.2-01 (excluding tracking devices from the definition of electronic communication).

303. *See supra* text accompanying note 298.

304. U.S. Telecom v. FCC, 227 F.3d 450, 453 (D.C. Cir. 2000); *see also* 47 U.S.C. § 1002 (1994 & Supp. V 1999).

305. *U.S. Telecom*, 227 F.3d at 463-65.

306. *Id.* at 464-65.

307. *See* H.R. 2975, 107th Cong. (2001) (suggesting amendments to the wiretap laws as a means to counter terrorism).

Department is leading the charge for greater capabilities.[308] The House of Representatives has gone so far as to title its provision PATRIOT (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism).[309] Since PATRIOT concerns amendments to the warrant requirement under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and not the industry assistance requirement found in CALEA, the law reviewed here is not fundamentally affected.[310] The law at issue is still binding, and American history teaches that concerns for liberty and privacy are always with us, even if more dormant in times of crisis than in times of peace and prosperity.[311]

Jason Broberg

308. Jesse J. Holland, *Senate, Bush Aides OK Anti-Terrorism Package*, CHI. TRIB., October 4, 2001, at 9N.

309. H.R. 2975, 107th Cong. (2001).

310. *Id.*

311. *Cf. generally*, Korematsu v. United States, 323 U.S. 214 (1944) (legitimating the exclusion and internment without trial of Japanese-Americans during World War II as a valid exercise of Congress' war power).

***